International Journal of Information Security (2024) 23:3065–3088
https://doi.org/10.1007/s10207-024-00878-0

REGULAR CONTRIBUTION

Trust management in the internet of vehicles: a systematic literature review of blockchain integration

Shirin Abbasi[1] · **Navid Khaledian**[2] · **Amir Masoud Rahmani**[3]

Published online: 5 July 2024

Abstract
The Internet of Vehicles (IoV) promises to revolutionize transportation in smart cities, but its interconnectedness raises critical security and privacy concerns. Limited computational power, diverse network technologies, and many sensors and vehicles challenge data integrity and trust in data exchange. Existing solutions, often dependent on specific environments and protocols, struggle to address these issues across the entire IoV ecosystem. This paper explores the potential of blockchain technology to address these challenges. We argue that blockchain's immutability and decentralization offer a unique solution for trust management in various IoV environments. We review existing blockchain-based algorithms and models proposed for IoV integration and propose a novel taxonomy to categorize these approaches. This taxonomy will help us analyze effective parameters, implementation methods, and evaluation metrics in the reviewed literature. According to our research, the most critical evaluation parameter for blockchain-based methods is time, including system-level service-related time parameters and solution implementation time, and 38% of existing papers simulated the approach using Hyperledger. Additionally, we will identify key challenges from integrating blockchain into the IoV landscape. By providing a comprehensive review and analysis of blockchain-based trust management solutions for IoV, this paper aims to contribute to the ongoing development of secure and reliable intelligent transportation systems.

Keywords Blockchain · Internet of vehicles · Intelligent transportation systems · Internet of things · Security

1 Introduction

Numerous services and applications were developed based on the growth of the Internet of Things (IoT). Intelligent transportation systems (ITS) built on the IoV are issues that have spread to the IoT. Connected vehicles collect data and transmit it to higher layers in these networks to access various services and applications. Data transfer poses unique issues because of network heterogeneity, different resources, node mobility, processing capacity limits on nodes, and multiple communication protocols. Trust management is an important topic because it involves a range of characteristics, such as security, privacy, and authentication. Various IoV trust management methods were presented, leveraging multiple technologies. Several studies focus specifically on one aspect of trust management. Reference [1] examines ITS security needs and dangers and classifies and evaluates solutions according to the communication and network levels. Many of the remedies are general detection and prevention measures. Another set of solutions that considers environmental characteristics and addresses the challenge of managing trust across all layers of the IoV is presented. Authors in [2] focused on security issues in IoV, discussing different methods based on artificial intelligence and blockchain in detail. They proposed architecture to support A.I. integration within IoV, but there are various challenges for data management and load balancing parameters.

The authors of [3] examined available solutions based on the environmental effect of data transmission. Blockchain technology is one of the tools used to manage the trust. One

✉ Amir Masoud Rahmani
rahmania@yuntech.edu.tw

[1] Computer Engineering Department, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Esch-sur-Alzette, Luxembourg

[3] Future Technology Research Center, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan

of the methods used to maintain trust in blockchain technology. Blockchain technology might provide a more straightforward solution to data transmission security problems. Researchers found that blockchain technology has emergent qualities, such as fault-tolerant computation and data sharing [4], that may strengthen trust in the IoV environment without violating resource restrictions. It lacks a single point of failure. Each block in the blockchain is equally authoritative, contains identical information, and ensures the immutability and trustworthiness of blockchain technology.

On the other hand, Trust management encompasses the processes and procedures that result in a trustworthy system. These techniques remove malicious nodes, defend against attacks, and prevent data manipulation. Authentication, security, and privacy are only a few trust management components. As a result of the IoV characteristics, trust management poses several complications. There are limited resources accessible to nodes. Due to their diverse structure and variety of security methods and protocols, trust management systems are susceptible to various attacks. Many papers were presented to cover these security requirements in different layers of IoV Communication [5]. Blockchain allows tracking transactions and data transmissions and provides data and resource management at the system level [6].

IoV environments require multiple vehicles to communicate with one another, and because the data is sensitive, strong security is needed. Blockchain technology offers clear transaction histories, decentralized consensus processes, and tamper-proof data storage, all of which can improve security. An assessment of current security measures and the holes they can fill with blockchain integration would be determined by a survey. IoV depends on trustworthy communication between entities. A survey would investigate the methods by which trust management models based on blockchain technology can evaluate the reliability of involved nodes. IoV devices communicate with each other according to how reliable the information is. The extent to which data in IoV systems can be trusted will be investigated by survey, mainly when blockchain is included.

To the best of our knowledge, no review article covers all of these steps, regardless of the various layers, services, and applications. This issue will be addressed in this paper. The contributions of this paper are:

- The steps for integrating blockchain and the IoV have been determined, and the relevant articles have been analyzed.
- The essential prerequisites and definitions of the blockchains are compiled and presented based on the environment's requirements and characteristics.
- Open challenges in the IoV and blockchain integration will be categorized and introduced.

In this paper, Sect. 2 will evaluate earlier works, Sect. 3 will examine the essential concepts, and the fourth section will examine the research methodology and questions. Then, in Sect. 5, we will analyze selected articles using the security, privacy, and authentication parameters. We will categorize and compare each parameter's evaluation methods, criteria, and parameters. We will classify the tools and algorithms and discuss the associated difficulties in Sect. 6. The paper concludes as described in Sect. 7.

1.1 Related work

This section discusses the resources and surveys related to trust management and blockchain technology in similar environments. At first, we examine the integration of blockchain and smart cities to understand the blockchain's characteristics better and adapt them to the requirements and challenges of the IoV. Bhushan et al. studied smart city security challenges and presented a blockchain-based solution [7]. The study examined the network and communication layers, the various protocols, and the classification of publications on communication security. Another research investigated the blockchain's potential to manage security challenges and its many applications in smart cities. IoV is referenced briefly in this article but is regarded pragmatically, with security considerations and trust management at several levels ignored. Numerous papers have examined intelligent transportation systems, whose foundation is the IoV [8]. The authors of [9] chose articles on blockchain and smart city integration published from 2016 to 2020, performed a bibliometric evaluation, and classified papers using keywords and methodologies. They do not, however, include the advantages or disadvantages. Furthermore, there is no categorization for the Internet of Things or linked automobiles.

In their paper [10], Srivastava et al. explored IoT dangers and assaults. They categorize cyber assaults and ways of detecting breaches and are concerned with security challenges from architectural levels. Moreover, the study evaluated blockchain technologies in terms of attack types. However, this article does not mention the various IoT applications or their unique characteristics.

Several researchers have focused on a particular domain of IoT. Elghaish et al. introduce the blockchain IoT (BIoT) as a novel fundamental concept [11]. The authors address the constraints and problems of this new paradigm and the numerous options for blockchain-based applications and services in the Internet of Things. They are particularly interested in smart cities and have restricted their focus to a specific target (building), where environmental aspects are often disregarded. This article is an excellent place to begin learning about the use of blockchain in the IoT.

Still, the articles are organized by technology and method, are sparsely reviewed, and do not include environmental requirements. Similarly, Hemmati et al. [12] have addressed the use of blockchain in the Internet of Vehicles. They have reviewed various applications for the use of blockchain in the IoV, and it is also necessary to add reviews in the field of simulation, parameters, and tools to this survey.

Some articles have restrictions on the structure and environment for review. Authors in [8] provided a comprehensive survey on blockchain and IoV integration based on environmental considerations and characteristics. However, they have limited their paper to specific communication and network protocols. Paper [13] deals with the Demand Response Management (DRM) of Electronic Vehicles (E.V.), in which some of the related challenges, privacy, and security are discussed. However, it does not deal in depth with the various solutions that cover them.

Authors of several papers concentrate on a particular component or aspect of security focus on data dissemination techniques [4, 14]. Bodkhe et al. [4] proposed a detailed review of traditional data dissemination methods. The authors discuss various aspects of data. However, resource limitations and different communication protocols are not taken into account. Reference [15] incorporates the Internet of Things with blockchain technology. They assert that blockchain technology may be used for communication and data management, hence combining IoT with blockchain technology for fault management. The blockchain stores IoT events and data logs for network and load balancing management, focuses on IoT applications, classifies attacks, and focuses on papers based on Quality of Service (QoS) requirements. The paper classifies attacks and manages privacy and security, emphasizing the communication and network layers. Papers are primarily categorized from the point of view of applications.

The blockchain is frequently used in distributed environments to manage resources and control non-functional requirements [16]. It was extensively used in the IoT, including IOTA [17]; some authors combined different technologies for solution design that they can benefit from each of them [18]. The authors take this further in reference [19] using blockchain to manage IoT security. They address significant challenges and issues related to security and compliance with regulatory requirements. The authors first classified IoT attacks and risks and then extracted security requirements. The first problem is that security gets greater attention in terms of trust than other concerns. Then, blockchain technology is reviewed, algorithms are examined, and IoT and blockchain integration concerns are addressed. Present approaches were categorized based on IoT applications and services, such as smart homes and healthcare. In this area, the IoV receives less attention; there is no statistical description, analysis, or review of current procedures. The writers do not try to discuss previous works' merits and flaws.

In [20], Liu et al. focused on evaluation criteria. However, they have also considered various applications of the Internet of Things and are not entirely focused on vehicles. For this reason, some aspects of this issue may not have been investigated because of the need for the Internet of Vehicles. It is also necessary to examine and study in more detail, other than the aspects related to quality parameters.

Kumar et al. [21] slightly improved the previous article by addressing additional trust management parameters. However, this research focuses on the IoT and does not analyze the various applications and their characteristics. Nonetheless, it examined the threats to the IoT from several perspectives.

According to the indicated evaluations, we thoroughly searched IoV, linked cars, and uncovered publications on the subject. We begin by analyzing the IoV's security difficulties and challenges, which are categorized according to their degree of security [1]. Various ITS-related attacks are first studied. Then, the multiple applications are assessed. This application and services were created to satisfy different functional and non-functional needs and the security concerns that come with them. When building solutions, security needs and dangers are taken into account. They are general and do not rely on any specific technology. The security side of networking difficulties is discussed in this article. Nevertheless, other critical aspects, such as data sharing and transfer, have been overlooked, while privacy and authentication have received scant attention. Moreover, the solutions are primarily classified based on security threats with overlooked environmental characteristics.

Therefore, the paper [22] discusses attacks on connected vehicles. This article summarizes all related attacks. These attacks are classified based on the system's general trust management requirements. The solutions examined primarily focus on predicting, detecting, and preventing attacks, and traditional solutions were investigated. There is currently no comprehensive analysis of blockchain methods in this field. Wang et al. [14] focused on security further by integrating the blockchain and IoV. This article discusses the various security solutions proposed for the IoV. Critical trust management factors are used to classify articles. Selected articles are categorized based on their intended use. The techniques' advantages and disadvantages have not been evaluated and classified, the problems with implementation and evaluation have not been investigated, and the present application difficulties have not been identified. Varma et al. also focused on a limited domain based on blockchain and SDN integration; they only reviewed

security issues and attacks, which can be expanded in future works.

Article [23] is presented in the IoV environment, but it has addressed the various applications of blockchain in this environment; it has mentioned security and trust management, but it has yet to address them in detail and has yet to cover its various aspects. Table 1 classifies papers according to their central topic and publication year. It summarizes these existing surveys and their differences from the proposed survey article.

According to the papers reviewed, the following weaknesses in the present survey papers were identified as follows:

- No paper covers all aspects of IoV trust management and comprehensively analyzes blockchain algorithms, methods, and issues on their simulation and evaluation parameters.
- No study covered all layers of the IoV, regardless of architecture, or considered the critical parameters for establishing trust in evaluating existing papers.

In this review paper, we try to avoid these weaknesses and cover the limitations of the research questions.

2 Background

This section proposes a taxonomy to review selected articles for using the blockchain for trust management in IoV, according to which the concepts are described in more detail. Finally, after reviewing the existing systems in this field, the above classifications are checked in each system.

2.1 IoV concept

The rapid advancements in science and technology have brought about significant changes in travel patterns and transportation systems through the Internet of Vehicles (IoV). The IoV utilizes vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to enable the exchange of information among vehicles. This dynamic data enhances safety, efficiency, and entertainment services, improving the driving experience [24].

According to the reviewed articles, a layered architecture can be thought of as follows in IoT and IoV: The first layer is the most fundamental, consisting of hardware, sensors, and nodes. Different types of vehicles and roadside units are interconnected [25–27]. As we see in Fig. 1, the sensors collect and transmit primary data to the higher layer. The second layer contains network communications, communication, and protocols, which define how nodes and higher layers communicate. The middleware layer is where the data source and management nodes are located. This layer considers cloud nodes, fog, and edges based on various policies and applications for applications [28].

Additionally, due to the requirement to pre-process and filter data for applications and services, this layer performs pre-processing operations before sending the data to the higher layer. This layer also manages data access and node identity. At the application layer, various applications are available to improve service to users and drivers. These programs are divided into programs that address user needs, environmental management, and non-functional environmental requirements. The business layer manages the business and ensures drivers and passengers receive the appropriate services. This layer collects data to manage business management challenges at a higher application level. Certain services are defined in this section.

2.2 IoV trust requirements and issues

Considering the various levels of trust in the system, the first level is trust between nodes. When necessary, nodes share data; thus, nodes must be trustworthy. This trust is typically established at the node or network level and ensures data integrity. This level prevents malicious nodes from interfering with communication and data transmission. Because these nodes transmit personal information, users' privacy must also be protected. Trust management at the service level requires data management critical performance and time parameters. At this level, resource management and security are also necessary. At the service level, data integrity must also be considered. Additionally, data and resource management must be ensured at all levels of the system architecture, including the physical, middleware, and applications and services levels.

The IoV collects data from the bottom layer, including multiple nodes, and transmits it to services and applications. This data includes, but is not limited to, user information such as location and health information, for which security and privacy must be ensured. The various security requirements are listed below:

2.3 Confidentiality

Unauthorized access to data or access by attacked nodes should be stopped so that the data access is controlled during transmission and only authorized services and nodes have access to this data.

Table 1 Studies related to blockchain and IoV integration for trust management

Paper	Main Topic	Advantage	Limitation	Our Contribution	Year
[11]	IoT and blockchain integration	The paper provided a general view of IoT and applications.	In many cases, it is not discussed in depth	We focused on essential parameters of trust management in detail.	2021
[7]	blockchain-based architectures, applications for smart cities	They examined all aspects of the blockchain concepts	No attention was paid to evaluating tools and parameters. Applications and services in the smart city were reviewed but not categorized.	we have more details and classification about methods on IoV, RQ1 and RQ2 for evaluation parameters and tools.	2020
[10]	IoT security challenges, attacks, and requirements	This paper provides a complete preview of attacks.	Privacy concerns are not considered.	We added privacy concerns and identified a more general perspective on trust issues	2020
[4]	Security challenges and requirements in data transmission on IoT	Security parameters and challenges for data are considered.	Network and architecture management should be added to the paper analysis.	In paper analysis, there is not only a data view, and all layers are considered	2020
[15]	IoT and blockchain integration for fault management in the communication layer	Not all aspects of the network and architecture are considered.	Only security issues are addressed, and some environmental constraints are not considered.	A broader scope was considered, and privacy and authentication were added to the analysis of the articles.	2020
[22]	VANET attacks, defenses, and solutions	They categorized all attacks.	Focused on security challenges based on attacks and the VANET environment	Different stages are considered both before the attack and after the attack. Moreover, privacy and authentication are added for analysis. Different architecture layers are considered.	2020
[19]	blockchain-based methods for security management on IoT applications	They focused on security issues for different applications.	IoV is briefly mentioned, and general parameters of the IoT environment are considered.	We added privacy and authentication to cover trust management. We updated parameters based on the IoV environment.	2021
[9]	Review blockchain-based methods on smart city applications and services.	All blockchain applications for smart cities have been studied in terms of technology and methodology.	There is no classification for challenges or concerns in vehicles.	We added a question for methods and solution classification on vehicles and focused on vehicles.	2021
[21]	Review blockchain-based methods for security and trust management on IoT	Authors overview different perspectives of security.	Tools and evaluation parameters are not considered.	RQ1 and RQ2 are added to classify parameters and tools.	2021
[14]	applications based on blockchain and IoV	The authors analyzed papers based on environmental characteristics.	There is no classification for blockchain-based methods.	We classified our methods into three different categories.	2021
[23]	applications based on blockchain and IoV	Papers are categorized based on their applications in IoV	Trust management concerns are not considered in detail	We focused on trust management in detail	2020
[8]	Blockchain and IoV integration for 6G environment	Security and privacy issues are identified on the network layer	No Method classification No authentication handling Limited to 6G	Trust management method classification No standard limitation Covers all layers of IoV	2022
[13]	Review blockchain-based methods for Demand Response management in IoV	It looks at the use of the blockchain in the IoV from a new perspective	No classification of the QoS. No identification of trust management	RQ1 and RQ2 for evaluation parameters and tools. We added security, privacy, and authentication for trust management handling.	2022
[20]	Review blockchain-based criteria on IoT	They focused on security and trust management criteria in blockchain-based methods in detail	They must cover another aspect of trust management. Their focus area is on different applications of IoT	All questions are designed based on IoV requirements	2023
[12]	Review on blockchain applications in IoV	They review various applications of blockchain in IoV	There is no question about evaluation tools or measurements	RQ1 and RQ2 for evaluation parameters and tools for more detail in blockchain application for trust management in IoV	2023
[16]	Blockchain and SDN integration for security improvement in Vehicular network	Attacks and security issues are classified and considered in detail.	They only focused on security improvement with SDN and blockchain. Their domain is limited	Trust management method classification No standard limitation Covers all layers of IoV	2023

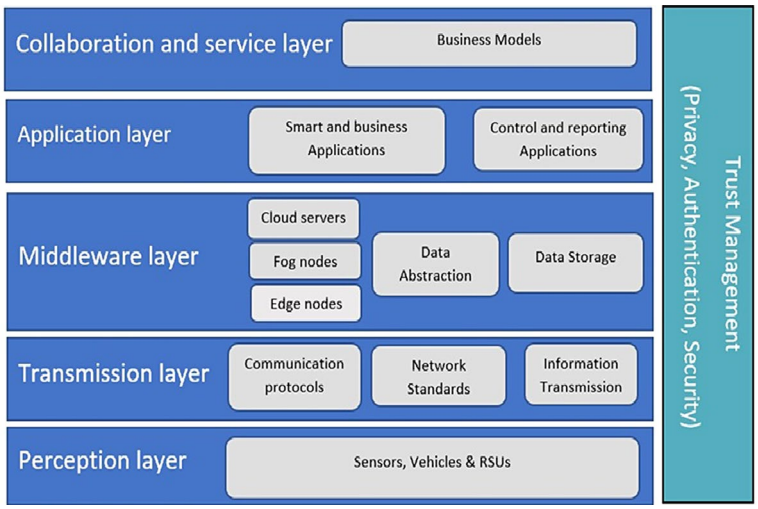

Fig. 1 IoV view with trust management [26, 27]

2.4 Integrity

The integrity of the data should be ensured so that it is not manipulated during the transfer, is correctly transmitted to the destination, and is guaranteed to be accurate. In this regard, it is necessary to manage network faults and even defective nodes to transfer data packets correctly.

2.5 Availability

Services must be available at different layers, and availability is one of the requirements considered in distributed systems.

2.6 Authenticity

The identity and authenticity of nodes and services must be verified to access and use information, and data access must have different levels based on their identity.

2.7 Non-repudiation

The sending node assumes responsibility for the data accuracy. The standards defined between sender and receiver are used to achieve this accuracy.

2.8 Forgery

Fake messages and data should not be sent to services and applications; it can reduce system-level faults and damages.

2.9 Data privacy

Much of the data is collected via sensors and provided to higher-level services and applications. Much of this data, such as users 'locations, is used in real-time services, and if users' privacy is not respected, users may refuse to send information and may not trust the services. Furthermore, some services are sensitive; for example, some services and applications are used to prevent accidents or alert emergency services, and if they do not have enough information, the probability of error can increase. Given the preceding, if we wish to classify the primary trust management requirements, Fig. 2 will be extracted:

2.10 IoV trust management challenges

Connected vehicles are at risk of intrusion due to the heterogeneity of connectivity and the increasing complexity of software, resource management, and computing [29]. Trust management encompasses the processes and procedures that result in a trustworthy system. These techniques remove malicious nodes, defend against attacks, and prevent data manipulation. Trust management includes several components, including authentication, security, and privacy.

Trust management presents numerous challenges as a result of the IoV characteristics. Nodes have a finite amount of resources. Trust management systems are susceptible to attacks due to the diversity of security solutions and protocols and their heterogeneous structure. Several types of attacks are detailed below [24]:

Confidentiality attacks Attacks on data confidentiality that enable unauthorized individuals and services to gain access to information that does not belong to them and for which the level of access is undefined.

Integrity attacks Manipulation of messages, injection of incorrect information, and transformation of data into

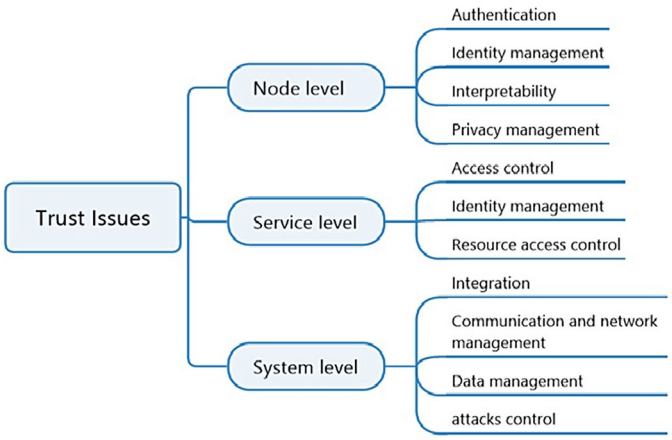

Fig. 2 IoV trust management requirements

incorrect data all pose a risk to system errors and costs using various techniques and at different layers.

Authentication and privacy attacks Fraudulent messages, information, and identities enable malicious nodes to gain unauthorized access to various levels or to exploit unauthorized identities, resulting in system-level errors and costs and interfering with service and user application processes.

Availability attacks Various attacks are launched against nodes, services, and the system, disrupting service operations and causing the system to fail.

Denial of Service (DoS) These attacks flood the system with requests, increasing its load, decreasing its response time, causing the system to fail, and preventing requests from being received and processed. If these attacks are distributed and utilize multiple IP addresses to attack the system level, they become more challenging to control.

Black-hole attacks Target packets and messages are lost in transit and never reach their destination. These attacks target packets and messages in transit, causing them to become lost and never reach their intended destination. One way to manage data packets and prevent these attacks is to add a sequential number to each packet at the destination.

Replay attacks These attacks repeatedly use valid data at inopportune times.

Sybil attacks In these attacks, forgery occurs, and users' identities are compromised, allowing unauthorized users to access data using the identities of others.

Impersonation attacks Malicious nodes attempt to deceive Roadside Units (RSUs) with false identities to gain access to and exploit various levels of information in this type of attack. This accomplishment can impact a variety of emergencies, vehicle congestion in a given area, and message prioritization. Encryption, data clustering, and localization can all be used to mitigate the effects of these attacks.

Malware attacks The resources to disseminate information about the IoV environment must be credible and reliable. Many services and applications fail to function correctly if these resources are attacked. Only data or messages from authenticated and validated sources will be accepted to mitigate these effects.

Timing attacks Because one of the characteristics of groups of services and applications in the IoV is their ability to respond in real-time, numerous attacks affect the time parameter. Services and applications experience a delay in receiving messages and data, resulting in their failure [30].

The attacks listed here are broad categories, each with a subcategory and occurring on various systems. Detecting IoV attacks is a significant challenge due to their node mobility and heterogeneity incorporated into new solutions [21].

Trust management presents numerous challenges as a result of the IoV characteristics. Trust management systems are susceptible to attacks in terms of the diversity of security solutions and protocols and their heterogeneous structure. Several types of attacks are detailed below:

Confidentiality attacks Attacks on data confidentiality enable unauthorized individuals and services to access information that does not belong to them and for which the level of access is undefined.

Integrity attacks Manipulation of messages, injection of incorrect information, and transformation of data into

incorrect data all pose a risk to system errors and costs using various techniques and at different layers.

Authentication and privacy attacks Thanks to fraudulent messages, information, and identities, malicious nodes may exploit unauthorized identities or obtain access to different levels without authorization. This leads to system-level faults, expenses, and disruptions in service and user application operations.

Availability attacks Various attacks are launched against nodes, services, and the system, disrupting service operations and causing the system to fail.

Localization attacks Malicious nodes attempt to deceive Roadside Units (RSUs) with false identities to gain access to and exploit various information levels in this attack. This accomplishment can impact a variety of emergencies, vehicle congestion in a given area, and message prioritization. Encryption, data clustering, and localization can all be used to mitigate the effects of these attacks.

2.11 Blockchain concept

Blockchain is the continuous chain of blocks that holds data in a distributed method. In reference [9], layered architecture is identified for blockchain; it consists of six layers. The data layer is placed on the bottom layer. Collecting data from multiple sources and data kinds and creating timestamps and metadata for data blocks are essential functions of this layer. The chain structure and data encryption rules will be specified at this layer. Next comes the network layer, whose main job is disseminating blockchain distribution rules across network-related nodes, services, and applications. This layer will define all communication mechanisms, confirmation/rejection mechanisms, and network protocol handling and will be critical for this environment due to the distributed structure of the IoV. Blockchain has many advantages for trust management in connected vehicles. User and vehicle data can be encrypted and securely stored on the blockchain, allowing authorized parties to access relevant information while maintaining patient privacy. Blockchain enhances data security and improves interoperability.

Moreover, it uses various techniques, including public and private keys and asymmetric encryption. The incentive layer is concerned with the mechanism for allocating resources. This layer determines the distribution of operations among different nodes based on their degree of participation and the policies established for resource management and cost management. The following are considered to be blockchain's primary characteristics [3, 8]:

Decentralization Transactions are managed in a distributed manner, which mitigates the risks associated with relying on a single point regarding cost, performance, and fault tolerance.

Non-repudiation All transactions are signed in the blockchain with a private key, and the other party confirms them with a public key.

Immutability The blockchain comprises interconnected blocks containing the previous block's hashed information. If the system is attacked, the changes made can be tracked.

Transparency The parties, their rights, and their authorized transactions are visible, simplifying the management of users and their information.

Regarding the characteristics above, it is possible to conclude that blockchain enables secure data transmission and communication among the nodes while ensuring privacy. This management occurs without the use of intermediaries or a centralized system. Reaching an agreement is one of the most important steps when using the blockchain, which various algorithms cover. Each algorithm has a specific usage. They are designed based on priority requirements.

2.12 IoV and blockchain integration

According to the articles reviewed, IoV trust management encompasses various parameters, including security, privacy, and authentication. The authors have worked on trust management requirements in different articles [31]. Multiple solutions were proposed for each parameter based on environmental characteristics. The authors [32] identified eight Critical Success Factors (CSF) to integrate blockchain and IoV in various domains, including functionality, performance efficiency, compatibility, usability, reliability, security and privacy, and maintainability and standardization. The articles we have analyzed look at this issue from different angles. In one aspect, these factors are considered as a requirement, and a service or application is considered [33]:

Data protection management Regarding the characteristics of blockchain, real-world data management requirements, such as access control, integration, data source identification, data compatibility, and data value optimization, are addressed. In decentralized environments, blockchain technology can facilitate data sharing and access control. Various system components are typically controlled in data management and sharing to prevent malicious nodes and

components from stealing critical system data and sending timely responses to services and applications [4].

Service management and coordination Various requirements are defined when designing applications and services at the IoV level. Several of these requirements are met by blockchain features, including reliability, emergency service availability, automated system management, and data privacy and security [19].

Resource management and allocation The blockchain IoV integration boosts system-level computation capacity and uses various mechanisms to motivate static vehicles to process data [8]. Some researchers work on performance evaluation parameters in services and applications.

Using blockchain with IoV, it is necessary to identify issues related to integration and their considerations. According to the reviewed articles, IoV trust management includes various parameters like security, privacy, and authentication. Different solutions were proposed for each of these parameters based on environmental characteristics. Specific difficulties and needs are offered for each of these criteria and solutions, which we will go through in greater depth in the following parts. After reading the articles [34], it is possible to classify the implementation tools and choose the implementation techniques. All the assessments agree that the identified existing sources are utilized to direct researchers with new ideas in this setting. In Fig. 5, the considerations related to the integration of the blockchain and the IoV are categorized, and in the following article, we will address each of them [35, 36]. The various branches of taxonomy will be completed via the different sections of the paper.

In the reviewed articles, the initial steps to determine the status of how to share data based on the definitions are designed, as well as steps for registering and determining the status of nodes, loading data, and generating keys to access

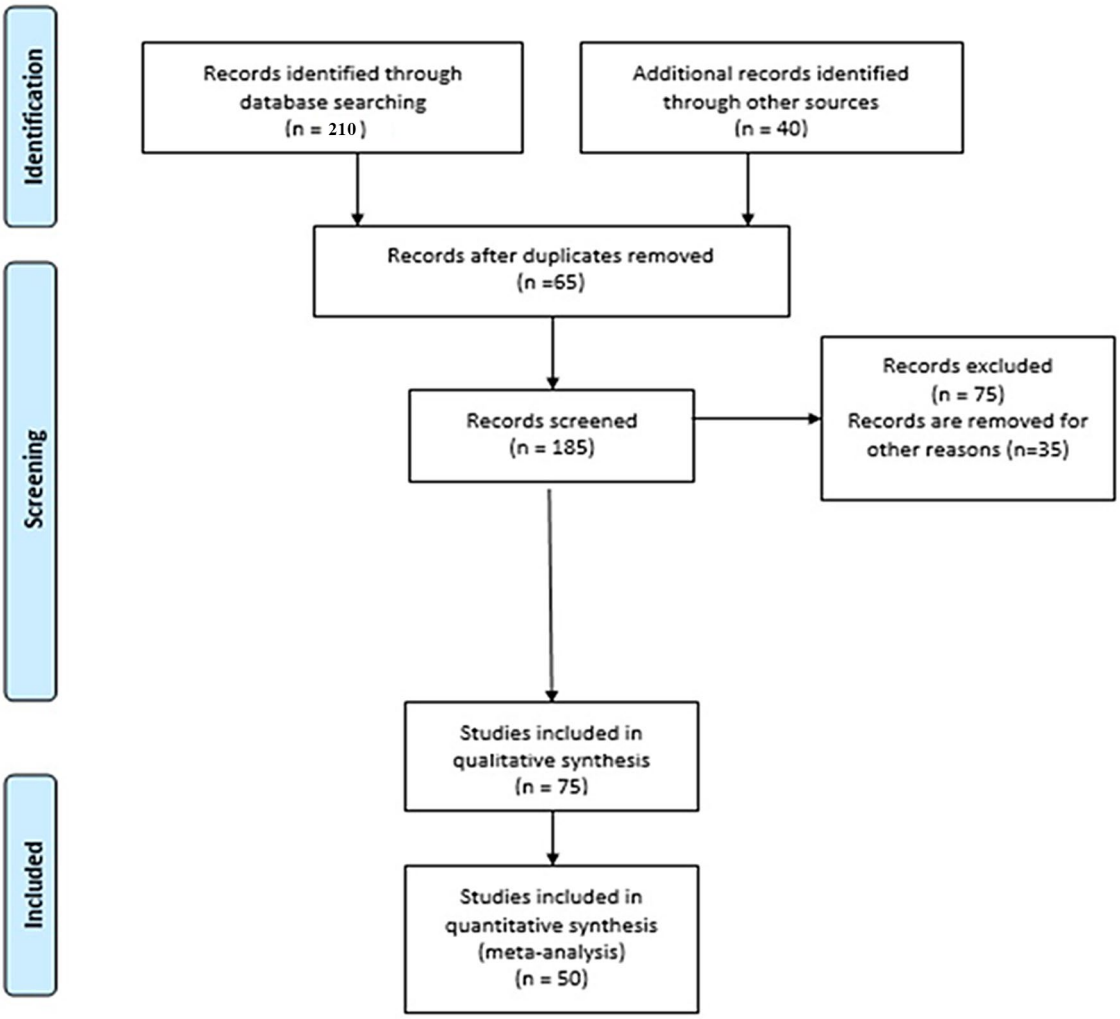

Fig. 5 Paper selection strategy

data. Moreover, security and certifying access to shared data are used when defining blockchains. The general steps in Fig. 3 are determined based on the nodes defined at different levels of architecture. This model will be more detailed in the analysis of the papers.

3 Research methodology

This section will define the research parameters, methodology, and paper selection. This method involves the formulation of research questions, the selection of databases, the definition of search terms, and the filtering of papers.

Fig. 3 A proposed taxonomy for Integration of IoV and blockchain for trust management

Table 2 Research questions

Index	Research Question	Reason
RQ1	What tools have been used to simulate and implement the studied methods?	There is no classification for evaluation tools on [8, 13, 14, 16] in the IoV environment. The simulations are very scattered, and this statistical information can be the starting point for choosing the best simulator according to the conditions in future research.
RQ2	What parameters are used to evaluate blockchain-based methods in the IoV?	Evaluation parameters are analyzed to determine which are more critical in trust management. There is no classification for evaluation parameters on [13, 14, 16, 23] on all IoV architecture layers. Categorizing these parameters can help improve existing methods in new proposals.
RQ3	What are the challenges and open issues of integrating the IoV and blockchain for trust management?	Open challenges will be presented for future work. Specific layers are considered for challenges on [8, 12–14], and we cover all layers. This question could be a starting point for future research.

3.1 Research questions

This paper addresses the following research questions in Table 2.

3.2 Terms and principles

The following search terms were used to find related papers:

("IoV" OR "Internet of Vehicles") AND ("blockchain") AND ("security" OR "privacy" OR "trust").

The principles considered to include principles are:

- Papers should be published in English.
- Journal papers will be selected.
- Papers were published from 2019 to 2024.
- Papers should cover different layers of IoV architecture.

The principles of exclusion are:

- Evaluation and simulation methods are ambiguous.
- The proposed method is designed as a service or application covering a specific IoV domain.

It should be noted that in different years, various articles have been presented in the field of trust management in the Internet of Things, which are not selected in this article due to the more general framework of the Internet of vehicles, as well as several conferences have been presented in this field and the recent three years [12, 20] that were not included in the selected articles due to the topic dispersion and the lack of use of conference articles.

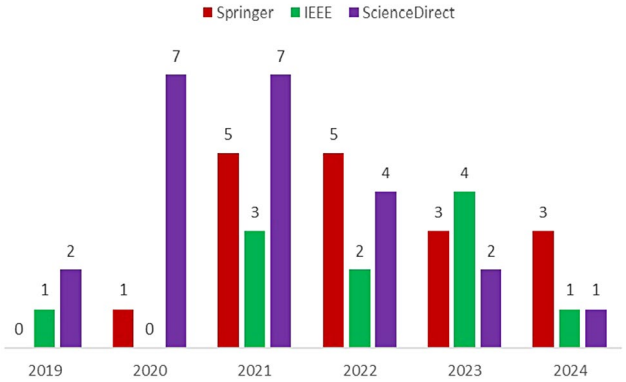

Fig. 4 Selected papers per database and years

3.3 Databases

Figure 4 represents selected publishers like IEEE, ScienceDirect, Wiley, and Springer, with paper numbers per database and year

According to the graph, the number of articles differs in different years. This number refers to the selected articles, and in each of the years, more research has been conducted that was not included in the selected articles due to the mentioned selection principles.

3.4 Research phases

We filtered our papers based on terms and criteria. Figure 5 details the steps to develop a search strategy and select papers based on the PRISMA Flowchart. In detail, we have followed the following steps to select the articles:

3.5 Data Collection and Selection

- We collected relevant papers from IEEE, Springer, and ScienceDirect. Our initial dataset consisted of 210 papers.
- We then applied inclusion and exclusion criteria based on Sect. 4.2 to narrow the selection to 50 papers that met our research objectives.

3.6 Taxonomy Development

- To classify the selected papers, we developed a taxonomy based on key themes and research questions in

Fig. 3. This taxonomy is created and categorized based on the view of Fig. 1.

- The taxonomy included trust management threats and attacks, trust management issues, trust management evaluation issues, integration issues and challenges, and trust management applications.
- We considered trust management threats and attacks, integration management, and issues in the background section. We classified selected papers based on trust management applications, and we analyzed these papers for evaluation parameters, tools, algorithms, and open issues and challenges.

Apart from the standards outlined in the acceptance criteria, we have read and classified the articles using taxonomy.

3.7 Data Analysis

Based on the definitions, those discussed based on system-level resources, communication, network design, bandwidth management, and information transfer during transmission are grouped into one category according to the View taxonomy. The second category is dedicated to data management due to the extent of attacks on data, the sensitivity of data, and their different levels. And finally, there is the third category, which covers the design for each situation with a bigger view.

4 Research classification

According to the extracted taxonomy, three general categories were considered for the methods. The first deals with methods that have provided trust management at the network and communication level; The second group has looked at data security and security and privacy at the data processing on the node level, and the final group has considered both node-level data processing and network-level security and methods. It is generally expressed at the system level. The initial degree of trust in the system, when looking at the many levels of trust, is trust between nodes. Nodes exchange data as required; thus, they must be reliable. Data integrity is ensured by this trust, which is often built at the node or network level. This level forbids hostile nodes from interfering with data transmission and communication. Users' privacy must be protected since these nodes convey personal data. Trust management at the service level requires data management, critical performance, and time parameters. At this level, resource management and security are crucial. At the service level, data integrity should be considered. Moreover, data and resource management must be ensured at all levels of the system architecture, including the physical, middleware, and applications and services levels.

4.1 Communication management-based methods

This section will examine communication management-based trust management methods for IoV based on blockchain technology. The first step is the authentication of two parties to establish trustable communication. Shi et al. [37] discussed distributed user management. It integrates blockchain and IoV. This article proposes a method that is scalable, secure, and decentralized. In this approach, trust management is delegated to edge and fog nodes. Communicating with the blockchain via this layer minimizes resource constraints on controlled sensor nodes, as is energy consumption. While this method ensures fault management and handling security, it is inefficient for real-time services that require immediate and sensitive responses. The ledger entities react to the Trusted Nodes' (T.N.s) requests. A TN wishes to connect with a to-be-trusted node (TBTN) with trust values. Reference [38] provided an overview of the blockchain. After registration, two-way authentication is performed (for sender and receiver). Afterward, the keys are updated, created, and exchanged, and data is transferred. This method uses various encryption techniques to ensure data transfer security, depending on the data sensitivity level. In the second communication step, the security of data transmission and the sending path must be considered.

In [39], a heterogeneous environment encryption system is proposed and implemented on the IoV. This system ensures data sharing security. Data manipulation is prevented using a blockchain, and data confidentiality is maintained. Considering the limited resources available in the IoT, non-certified encryption at the node level was used to avoid increasing network load and node computations. A layer in the proposed system model comprises fold blocks and intelligent nodes. The nodes' private data are encrypted on the cloud layer, and blockchain technology regulates access to these levels. Before they may access the data, both nodes and services must authenticate. This is how a crucial generation center generates the system keys. Hence, the nodes communicate with one another using public keys while maintaining their anonymity. A node participates in the data query process in this technique, which involves storing and confirming the validity of the most recent block data, which is used to decide when modifications should be made. This may raise the chosen node's operational complexity and risk, demanding a solution to enhance it in future work. This approach exceeds prior methods regarding cost, energy usage, performance, and time factors. In [40], a blockchain-based method for communication security at the

system level is presented. This method uses batch authentication for the nodes. This method provides greater security than batch authentication of messages, as security solutions are implemented at system and data levels. The cluster nodes are examined in the first case to authenticate nodes in batches, and each node can verify its neighboring nodes at the cluster level.

Paper [41] deploys blockchain technology on cloud servers. The blockchain manages each node's cost information and storage requirements. On the other hand, each node is authenticated using the same method. The agreement key is used to communicate messages among the nodes. The nodes' positions determine this key; consequently, the nodes' mobility is also covered. The cloud layer has several trustworthy sources responsible for establishing and maintaining blockchains. This method is evaluated using security parameters and examines which attacks are covered, which security issues were addressed, and how much improvement was made. Singh et al. [42] proposed a blockchain-based approach to ensuring trust and security in peer-to-peer networks. Apart from the fact that this technology is similar to ITS, intelligent vehicles were used to evaluate the method. The proposed method uses a local dynamic blockchain to ensure secure communication among the nodes, a master blockchain to manage and track data, and a secure encryption method designed for system nodes' security and reliability. In the paper [43], the authors proposed an authentication scheme based on blockchain for empowering security in intelligent 5G IoT. This scheme worked on the four layers of cloud computing architectures. As evidenced by the reviewed articles, most articles at this level deal with nodes, the network's physical and communication layers, and the security of hardware and infrastructure. The following section will discuss data management security, trust, and privacy. One step further, Vishwakarma et al. [44] used a consensus algorithm suitable for the MPBFT consensus scheme in a hybrid SDN-based architecture that prevents insecure access and communication. They added authentication and cryptographic algorithms in message transmission for security improvement. It may cause scalability and latency issues due to the large number of transactions in the real network.

4.2 Data management-based methods

This section reviews data management-based IoV methods implemented based on blockchain and IoV integration.

Numerous papers use encryption to safeguard users' data privacy. Paper [37] proposed a blockchain-based data-sharing protocol for vehicular social networks. They use cryptography to conceal nodes and users' identities and blockchain technology to prevent data manipulation. Multimedia data are of great relevance to them. The responsibilities of trusted authorities, electronic vehicles, users, RSUs, and blockchain are all investigated for system analysis. A system model based on these responsibilities has been developed. Attacks and potential threats have been examined and classified for each. However, it is necessary to ensure that no one except the recipient, sender, and authorized users has access to the data to prevent data access. This access control is implemented at the data loading, updating, and usage stages.

Furthermore, traceability is added to the system to detect malicious nodes. Records of messages received/sent and data about the sender and receiver are kept under a pseudonym, which can be used to conceal users' identities from potential attackers. The block's data keeps track of and produces further information. The temporal parameters employed in this work are those connected with several phases of data management, such as the beginning stage, data sharing, blockchain formation, and updating. However, there is no requirement for real-time reaction at the system level. It is necessary to compare security parameters to determine the effectiveness of the proposed method to protect individuals' privacy. Paper [45] uses blockchain technology and appropriate blind signatures. This system trusts the message if the number of signatories does not fall below a predefined threshold. Control mechanisms can determine the sender's identity if the message is malicious. One issue with this method is that using a signature mechanism and a certain threshold depends on the number of nodes and the area covered. It means that if the number of nodes is small or scattered, it affects time parameters, increasing and making responding to services more difficult. The article's evaluation considers the cost parameter but is not a comprehensive evaluation method for security or privacy.

Several solutions cover data security by combining solutions based on various technologies. Zhang et al. [46] proposed a blockchain-based protocol to generate an asymmetric group key protecting user privacy. The protocol's nodes are anonymous, and data is exchanged using a public key. This strategy distributes and balances the computations across the nodes because of the characteristics of the IoV and the limited resources present in the nodes. This technique may be enhanced by solving the problem of service responsiveness, ensuring service quality is constant regardless of protocol complexity and length, and producing blockchains. To this end, various service parameters must be considered. In paper [47]. The data is encrypted in the blockchain and is accessible only to authorized users. A system for data management was suggested by Wang et al. [48]. Vehicles in this system collect environmental data and subsequently upload reliable data to neighboring RSUs. They created a deep learning-based verification model to

determine the reliability of uploaded messages, determine the credibility scores of vehicles based on the results, and identify malicious vehicles per the findings to stop malicious vehicles from uploading fraudulent messages. This work combines deep learning and blockchain technologies to create a trust management system for connected cars. The proposed system will include vehicles and RSUs in the trust management process and calculate the trust level of the data that vehicles upload to assist in deciding the degree of trust that vehicles have.

Karim et al. [49] studied various attacks and security challenges in IoV. They suggested a blockchain-based data exchange scheme that uses the Elliptic Curve Cryptography algorithm. They also developed an authenticated key agreement scheme that relies on blockchain. A block created is sent to the leader node, chosen from the RSUs group. The leader node verifies, validates, and adds the block to the blockchain network, with the help of the blockchain center, by using the Practical Byzantine Fault Tolerance consensus algorithm. This method has low computation and communication costs. However, it may have scalability and latency problems due to the network's many vehicles and transactions. Tu et al. [50] proposed a vehicle-based secure blockchain consensus approach. This method includes some procedures for data and transaction validation on the blockchain. The authors designed an authentication approach and a key distributing and request process for vehicle authorization for blockchain updates. Real-world scenarios must be considered for time parameter evaluations.

Article [51] has also done similar work, with the difference that it has also worked on the issue of cost awareness and scalability and has used lightweight techniques for authentication for this purpose.

Devi et al. [52] suggested a blockchain-based vehicular architecture that can provide a reliable, optimized, secure, and trusted solution to address the security challenges of vehicular networks. They designed a blockchain-based trustworthy framework for vehicular networks that has three main parts:

1. A trust evaluation model that uses the DPSO algorithm to measure the trustworthiness of vehicles based on how they behave and interact.
2. a trust update model that uses the M-ITA algorithm to adjust the trustworthiness of vehicles based on the feedback from other vehicles and the blockchain.
3. a blockchain-based data storage system that uses the PoT consensus protocol to store and verify the trustworthiness of vehicles in the blockchain.

This framework can support real-time services but requires high computation and communication resources because of blockchain and complex algorithms. For this problem, Yuan et al. [53] proposed a blockchain-based trusted data-sharing mechanism with congestion control in IoV. They designed the Kademlia algorithm-based traffic data forwarding method to control channel congestion state. Their approach reduced communication and network overhead, but privacy was not considered.

At the cloud layer, solutions are developed to verify that data are accurate and originated from the correct source. The data is encrypted in the blockchain and is accessible only to authorized users. After encryption at the destination, messages are sent to RSUs. These units are used to determine the legitimacy of the data sender node. The senders or recipients of the message are not identified in this method. The system stores their nicknames to prevent a third party from identifying the nodes. This method uses mass message confirmation to reduce communication costs, ensuring the node's legitimacy approves all sent messages. Costs are cut, but a minor increase in security risk results. The data transmitted by illegal nodes may be extensively validated in the case of an assault since all roadside units, in particular, are regarded as insignificant. Security criteria are used to evaluate this method and determine whether it meets its objectives. These goals are based on the identified security risks. Temporal parameters are used as quantitative parameters to compare this approach to others. Several studies look at data management policies across the board. Khalid et al. [54] described a blockchain-based data management system. This strategy uses blockchains in roadside units due to a lack of resources. Event-based validation is used in this system. Based on events, the data is separated into smaller packets. The appropriate modifications to the blockchain are performed after checking their authenticity, and the information connected with the occurrences is saved in the blockchain.

Furthermore, data addresses are stored in blockchain-based contracts, preventing data redundancy. The system's analysis is based on its resistance to attack. The certificate is created with the node's original identity, resulting in network disruptions during system-level attacks. The source announces the event and initializes its properties. Witnesses sign the events, and the source acts as a witness to verify their signatures.

Furthermore, the event information is sent to the roadside units after verifying the witnesses' authenticity and updating the blockchain. The paper does not specify a method for selecting roadside units, limiting scalability. Singh et al. [55] proposed a deep learning-based blockchain scheme for security improvement in smart cities. They pay attention to cost management as a challenge in the IoT environment and optimize energy consumption in resource management.

The primary purpose of data management and retention was stated in the paper [56]. Even in the article's evaluation, the primary parameters include data retention parameters; however, the certificate issuer stores the nodes' aliases in this method. It sends messages encrypted in the checkbox, which increases the system's privacy, and this method ensures that no virtual access to an individual's identity can be used to manipulate it due to the miner's selectivity, resulting in improved system security. However, the article contains no criteria to maintain these parameters. Furthermore, scalability is not considered in this paper.

The authors of [57] proposed a blockchain-based scheme. They are primarily concerned with data management. This method begins by detecting malicious messages. Their priority for sending and receiving messages and creating, using, and updating the blockchain falls as their sending nodes' trust score rises. To prevent assaults, they are not allowed to enter roadside installations. Even so, they have to be taken into account for larger-scale applications. In the paper [58], the authors covered scalability. They proposed a blockchain-based architecture for the Internet of Things, which focuses on managing information exchange in different layers and ensures data security and privacy preservation. In the cloud layer, the authors used the Hash Data Table. Reference [59] proposed a framework based on blockchain technology that focuses on message reliability during transmission. The sender and receiver nodes are authenticated first in this protocol. The proposed system model incorporates direct registration of roadside units and connectivity to cloud servers. A system node is clustered and registered with the nearest roadside unit, and cloud servers confirm each node's registration with the nearest roadside unit. Prioritized messages are sent, and data blocks are created utilizing this information to authenticate nodes. The system's performance and resilience to assaults are evaluated to test this technique, and the findings show that transparency and confidence are ensured in various security situations. However, the scalability and temporal factors crucial to the IoV have not been examined at the service level.

Another study introduced a consensus method called driving proof and a technique to select miners based on service-based filtering [60]. The first time a vehicle enters the network, it is detected. Blocks are constructed using this critical information. The authors of [61] develop a reference model for data management in IoV systems. They incorporate blockchain technology into their Generated Data Protection Regulations (GDPR). They primarily focus on data security, risk analysis, and storage allocation management. The first layer, which contains tools and sensors, is defined in this article as a three-layer architecture. The infrastructure, communications, and protocol specifications are described in the next layer. This layer defines and maintains blockchains. The following layer is services and applications, defining encryption and decryption services. One of the benefits of this design is a faster response time to services due to the service layer's definition of control mechanisms.

Moreover, real data were used to simulate this method. Testing the system's scalability in subsequent works is preferable to determine whether it maintains cost and performance even at high volume. As evidenced by the reviewed articles, one group of articles is designed around reliability requirements, while another group manages data at various architectural levels, if not the entire system. The issue is that infrastructure and service response has failed to provide a feasible solution on a large scale and in adverse environmental conditions. Consequently, the following section examines solutions that consider some of these parameters.

According to the reviewed articles, the primary concern of blockchain-based solutions in data management is data access and data updating by unauthorized people in the system.

4.3 System management-based methods

This section will discuss system management approaches that are based on blockchain. Several researchers develop frameworks or schemes encompassing the entire system and a subset of critical environmental parameters. A study [62] proposed a framework based on the blockchain to ensure the security of system-level transactions. Previous methods relied on all RSU nodes to create and update blockchain information. However, this framework uses the POAT algorithm to avoid excessive energy and cost consumption due to the environment's limited resources. This framework selects miners from the cloud and RSU nodes with a high level of trust as miners. The level of trust is determined by the legitimacy of the node's transactions. This level of trust is updated during transactions, and it can be used to detect attacks even when an RSU is operating normally.

A redundancy technique accounts for the node's mobility, one of the system's primary characteristics, and ensures the data's accuracy. This method outperforms previous methods in terms of performance and cost; however, due to the larger scale and faster response time to real-time service solutions, improved methods for controlling the trust level and the number of messages transmitted in the system should be added to the framework. The IoV's network name and blockchain architecture are combined in Paper [63]. Data naming networks have been employed in the IoT to get around IP-based networks' drawbacks. The architecture of these networks makes them ideal for data-driven services. One of the problems with these systems is that they do not cover all services, which should be assessed in future

research. The article suggests blockchain-based solutions for these networks to guarantee security. In this architecture, the blockchain comes after the infrastructure layer and comprises two main components: the data and header blocks. The header block contains control information and metadata about the source data and is used to perform the necessary controls. This article does not mention simulation, and essential criteria, such as scalability and time parameters, are omitted.

Paper [64] is similar to the paper outlined above. This study discusses authentication for the sender and receiver and anonymous message transmission. Unlike the previous article, this one considers various system models and scenarios for simulation, and because resources are limited on the IoT, time and processing parameters are evaluated. Paper [65] discusses the IoV features required for a lightweight Internet. This study presents a broad strategy and methodology to solve this restriction. This work considers the processing capability and constrained memory management of nodes. This design takes advantage of mutual authentication. Paper [66] proposes a new architecture for the IoT based on a hybrid of blockchain and quantum. The architecture comprises three major components:

- Quantum communications for information exchange among nodes, servers, and roadside units;
- A blockchain for data management, control, and analysis;
- The issuance of new results.

In some papers on system design, other considerations besides trust have been considered. In an article [67], Rahman et al. have presented a new design of systems based on 5G networks, which can be extended to the Internet of Vehicles. This design uses a combined method based on blockchain, machine learning, and SDN technology. In this method, in addition to providing security through blockchain, using machine learning algorithms, the bandwidth used at different times is predicted at the system level, and for this reason, resource management is also improved, but the implementation of this Due to the use of different techniques, the method has high complexity and cost, and time parameters should be checked in its design.

Paper [68], the creation of an ID is used for authentication to protect privacy, and this ID is used to create a session between vehicles. In this article, a blockchain-based distributed smart contract system is designed to use RSUs for certificate-based authentication. This method reduces the overhead at the system level and during information exchange. It is necessary to consider time parameters for support in real-time systems.

A study [69] proposed a blockchain-based framework for securing intelligent vehicles. The proposal concerns increasing vehicle attacks regarding process automation and more intelligent vehicles and road equipment. It is intended to prevent attacks that disrupt system performance due to unauthorized access. Secure communication and access control are the focal points of this approach. The essential advantage of this approach in the IoV context is that it gives acceptable reaction time, which is crucial for real-time applications.

As noted in most articles' analyses, one of the significant obstacles in installing IoV blocks is achieving the services' time and performance requirements. The paper [70] provides a location-based data access control technique for IoV to improve the performance of these methods; in this strategy, the data originator encrypts and uploads its data to the cloud server. Fog nodes are designed to provide authentication options for managing data access. This includes specific node-specific characteristics (attributes, location, period for access). The user location monitoring method is used to update information and issue keys. The nodes should be deployed at their respective locations to receive the key, verify it, and access the data. They are highly effective. However, time parameters are not considered. In [71], the authors propose a solution based on reputation. Therefore, this article discusses the service's quality parameters and the environment's characteristics. This may include the difficulty associated with responding to real-time services. In [72], the authors proposed a deep learning and blockchain-driven security framework for 5G-enabled IoT environments to cover all layers in IoT environments. This method has acceptable performance and reliability in the simulation scenario. Cheng et al. [73] developed a conditional privacy-preserving authentication scheme that uses the identity-based signature (IBS) algorithm for vehicle authentication in a 6G environment. They designed a pseudonym management scheme based on blockchain for security improvement. This method allows the authority to trace the real identities of the vehicles and the RSUs under certain conditions. For future works, scalability must be considered.

The proposed method in [74] has four phases. The network topology information is analyzed, and the enemies are identified by determining the reliability parameters at the network and system level and the cost and time parameters. The initial model is designed.

The proposed model starts by calculating the trust values of the nodes. After calculating the trust values of the nodes, the model selects a validation node using a selection algorithm. Then, Byzantine fault tolerance selects a speaker node, and the others act as representatives. The speaker then verifies the claims, creates a hash, and then sends the proposal to the delegates. Delegates also review and compare

a speaker's results with those of delegates. If the results match, the block is created; otherwise, the request will be dropped. After the block is generated, the model verifies all transactions. In addition, the model uses the Batman routing protocol to find the best next hop and forward depending on the specific hop. Adapting blockchain to MANETs involves addressing the extreme computational complexity of block validation. Balancing this complexity while preserving blockchain characteristics is a challenge.

As mentioned in the discussed articles, a group of articles has improved reliability at the data, communication, and system level using hybrid solutions and blockchain. The reason for using other solutions is to cover other quality parameters. Also, in most articles, the system's performance has been measured along with security and safety, and it is necessary to create a compromise point.

Table 3 categorizes the methods and simulations used in the papers, compares the parameters associated with blockchain implementation at the IoV, and describes the attacks covered.

5 Results and comparison

This section analyzes the present blockchain-based trust management methods in the IoV context. The analytical reports are based on the following questions:

According to the papers reviewed, methods can be classified as data management-based, communication management-based, or system architecture-based. The first category includes techniques for transmitting, distributing, and managing data that are more directly tied to the middleware layer. Another group oversees communications and network security, while another oversees all architectural levels.

As shown in Fig. 6, most papers are in the data management solutions category. This problem stems from two issues. The first issue is data's significance in addressing security and privacy challenges. Data will significantly increase system reliability if appropriately managed by preventing attacks and unauthorized access to valuable data. Furthermore, the transfer and exchange of information among all layers of the IoV architecture raises system management risk and necessitates control strategies to counter-attack attacks.

We classified the selected paper based on the corresponding author country and continent in Figs. 7 and 8. As expected, developing countries and developing regions work more on these issues.

5.1 Simulation tools for blockchain and IoV integration

RQ1: What tools have been used to simulate and implement the studied methods?

According to Fig. 9, Hyperledger is used for 38% of paper implementation. Furthermore, 13% of papers used the Ethereum tool to assess and analyze existing case studies. Some authors failed to specify a tool for evaluating their methods.

5.2 Evaluation parameters for IoV and blockchain integration

5.2.1 RQ2: what parameters are used to evaluate blockchain-based methods in the IoV?

The meaning of cost in the diagram below is the subject of resource management at different levels, including communication, network, system, and computing costs. Energy consumption management is also included in this group. Moreover, the discussion of time is raised regarding specific time parameters for services, including response time or time parameters related to blockchain, such as transaction time. The parameters related to fault tolerance mean the success rate in error and attack detection, and the performance parameters refer to time parameters affecting the entire system, real-time response, overhead control, and complexity. Figure 10 is derived from the evaluation section of the reviewed articles.

For future work, it is suggested that models based on trust control, presented in different articles, be used in addition to general criteria. The parameters are selected in these models based on the system's primary needs. The dynamic trust model addresses the specific challenges of the IoV. These parameters are defined based on the environmental needs and change based on the selected criteria. In the following equations, equations based on trust are defined and designed based on different requirements [76]:

Fuzzy Trust Model: The Fuzzy Inference System combines linguistic rules with numerical data to make decisions. A simple equation for fuzzy trust aggregation could be:

$$\text{Trust}\,(i) = \frac{1}{k}\sum_{j=1}^{k} \text{DS}(j,t) - \text{DS}(i,t) \tag{1}$$

DS (j, t) represents the trust value of every node (i) at the time (t), and k is the total number of nodes in the system.

Bayesian Trust Model: Bayesian probability theory is often used for trust modeling. It

Table 3 Blockchain-based trust management papers comparison

Ref	Simulation tools	Blockchain approaches	Attacks addressed	Trust parameters	Evaluation parameters
[37]	Hyperledger Fabric	Permissioned blockchain and consensus algorithms	Fault in nodes	Access control, integrity	Scalability, cost, and error detection
[62]	NS3 for nodes network generation, Hyperledger Iroha	PoAT algorithms and private blockchain	Sybil attacks, DDoS attacks	Access control, Privacy, Authentication	Energy consumption, success rate
[31]	Public chain Ethereum	public blockchain	Malicious attacks	Access control Privacy Authentication Integrity	Error detection
[47]	Not considered	public blockchain	replay attacks	Access control Privacy Authentication Integrity	Cost management, performance
[56]	MATLAB	public blockchain	Sybil attacks, dictionary attack	Access control Privacy Authentication Integrity	Time parameters
[41]	AVISPA for security evaluation	public blockchain	Eavesdropping attack, replay attack, Trust authority, impersonation attack	Access control Authentication Integrity	Cost management
[40]	Hyperledger Sawtooth	PBFT algorithm and public blockchain	Sybil attacks, double-spending attacks, mining pool attacks	Access control Authentication	Attack detection, performance
[54]	Python, solidity language, and Ethereum platform	PoW algorithm	malicious attacks, replay attacks	Privacy Authentication Integrity	performance
[38]	C++ & Crypto++library	PBFT algorithm and public blockchain	DDoS attack, replay attack, identity theft attack, traffic analysis attack	Access control Privacy Authentication	Error detection
[39]	MICA2	Public blockchain	Not considered	Access control Privacy Authentication Integrity	Attack detection, cost management
[56]	Ethereum platform	PoW & PoS algorithms	Data tampering attack, Algorithm tampering attack	Access control Privacy Authentication	Performance, error detection
[64]	Not considered	PoW algorithm and permission blockchain	DDoS attacks	Access control Privacy Integrity	Cost management, time parameters
[66]	Not considered	BFT and NBFT algorithms	replay/relay attacks, user impersonation attack	Access control Privacy Authentication	performance
[42]	Not considered	PBFT algorithm and local dynamic blockchain	DDoS attacks, Malicious attacks	Access control Privacy Authentication	performance
[69]	CORE	public blockchain	Fake data, Code injection, Sybil attacks, Malicious attacks	Access control Authentication Integrity	Attack prevention, performance
[46]	Cryptographic library MIRACL Ethereum	PBFT algorithm and sharing style blockchain	Fake data and messages	Access control Privacy Authentication	Performance, time parameters
[60]	JAVA SE	PoD algorithm and permission blockchain	Fault attacks, Malicious	Privacy Authentication Integrity	Fault detection
[61]	Not considered	Private blockchain	Misbehaving Vehicles	Access control Privacy Authentication	Performance, attack detection
[70]	--	private blockchain	malicious attack, cyber attacks	Access control, privacy Authentication	Error detection, performance
[72]	Tensorflow, Ethereum	Private blockchain	Malicious attacks	Privacy Access control	Performance, time parameters

Table 3 (continued)

Ref	Simulation tools	Blockchain approaches	Attacks addressed	Trust parameters	Evaluation parameters
[55]	Not Considered	consortium Blockchain	Malicious attacks	Privacy Access control	Energy consumption management
[58]	SUMO, OMNeT++, Ethereum	Private blockchain	integrity attacks	Privacy Authentication Access control integrity	Attack detection, performance
[111]	Hyperledger Fabric	consortium blockchain	Sybil attacks., Collision attacks, Fault attacks	Access control Authentication Integrity	Performance, time parameters
[48]	SUMO	PoT	Not considered	Access control and valid information	Performance
[66]	MATLAB	PoT	DoS attacks, Sybil attacks	Privacy, Authentication	Performance, attack detection
[44]	JAVA	MPBFT Consensus Algorithm	impersonation, Sybil, man-in-the-middle attacks	Confidentiality, integrity, and authentication	Performance, cost, and time parameters
[53]	Python, Ethereum	Private blockchain	Collusion attack	Authentication, integrity	Time parameters, Performance
[49]	C, C++and MIRACL	consortium blockchain	Different types of attacks are considered.	Authentication, Privacy, Access control	Time parameter, Cost, Performance
[68]	NS2	PoT	Different types of attacks are considered	Authentication, integrity	Cost, Performance, Verification loss rate
[73]	Hyperledger	consortium blockchain	man-in-the-middle attacks, replay attacks	Authentication	Time parameters, Cost
[75]	OMNET++, SUMO	PoS	DoS attack	Authentication, access control	Attack detection, performance
[74]	NS3, C++	Consensus Mechanism	Not considered	Access control	Attack detection, performance
[67]	Ethereum, Wireshark	PoW	Malicious attacks	Access control	Success rate, performance, cost

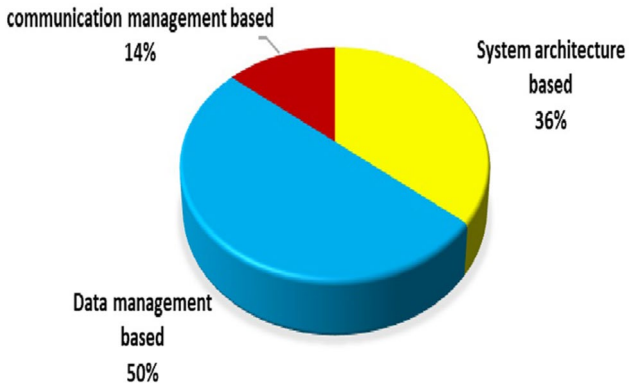

Fig. 6 Blockchain methods for IoV and blockchain integration

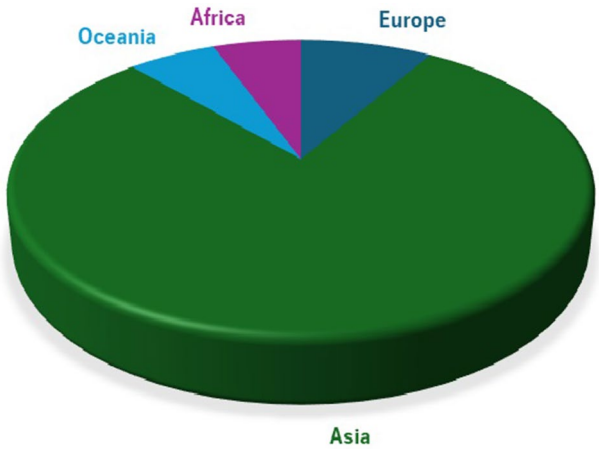

Fig. 7 Selected papers based on continent

represents dependencies between trust factors. The Bayesian updating equation for trust could be:

$$UpdatedTrust\,(i) = \frac{PriorTrust\,(i)\,.Likelihood\,(i)}{Evidence} \quad (2)$$

Prior Trust (i) is the initial trust belief. Likelihood (i) represents the likelihood of new evidence supporting or contradicting the trust, and evidence is the total evidence available (Fig. 9 and 10).

When determining trust models, the following considerations should be identified:

- **Dynamic Trust Update**: Trust evolves due to changing interactions and behavior. Recursive equations or dynamic models update trust values based on new

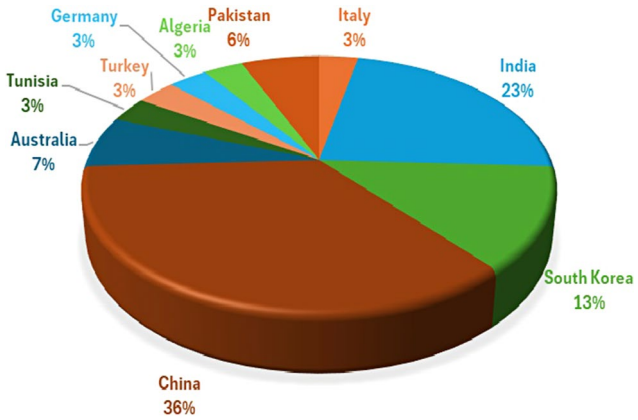

Fig. 8 Selected papers based on the country classification

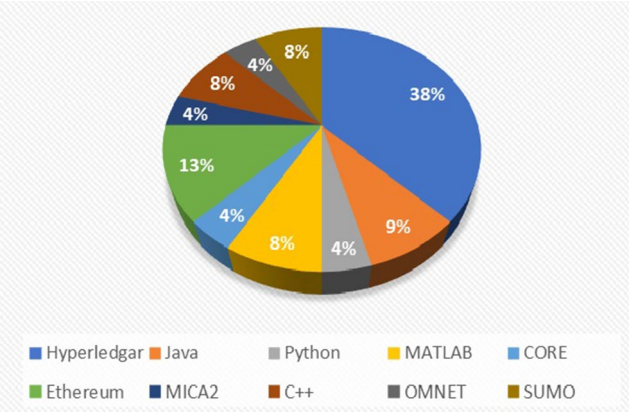

Fig. 9 Simulation tools for IoV and blockchain integration

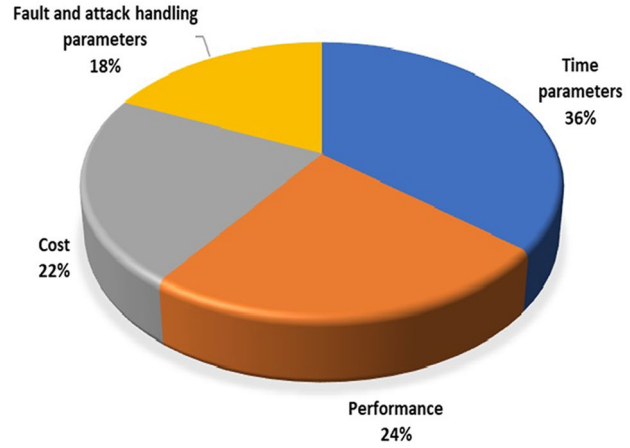

Fig. 10 Evaluation parameters for IoV and blockchain integration

evidence. A function can identify that updates trust based on the latest interaction:

- **Threshold-based Trust Decision**: Trust thresholds determine when to trust or distrust a node. Decision rules guide trust decisions.

When evaluating the performance of trust models, several parameters and metrics are commonly used:

- **Precision**: It measures the proportion of correctly identified positive instances (true positives) out of all the cases predicted as positive.
- **Root Mean Squared Error (RMSE) quantifies the average difference between predicted** and actual trust values. Lower RMSE indicates better accuracy.
- **Average End-to-End Latency**: It represents the time data travels from source to destination.
- **Packet Delivery Ratio (PDR)** calculates the proportion of successfully delivered packets. Higher PDR indicates better reliability.
- **Throughput**: it is identified for measuring the data transfer rate.

5.3 Open issues and challenges

5.3.1 RQ3: what are the challenges and open issues of integrating the IoV and blockchain for trust management?

The following points should be considered when merging the blockchain and the IoV:

Delay-constraint application and services Security is built into several IoV services and apps. Regarding the stated tiered design, they need data to be received from the bottom layer at a specific time. Responsibility for these services is specified in real time [8]. Data and message transmission may be delayed if defensive measures are deployed based on the environment's characteristics to protect security and privacy. This problem must be considered a compromise in the system to prevent service failures.

Scalability This is one of the issues not addressed in most papers reviewed. Many methods discussed in the articles impose a high cost on the system regarding time and computation when implemented on a large scale. Given the limited computational resources available and the requirement for real-time response in some services, this is one of the issues that should be considered [75].

Complexity Miners should choose a solution and consider the amount of trust and data security techniques like encryption since various consensus algorithms are utilized to build and maintain blockchains. The suggested solutions are coupled with increasing tool and computational complexity due to environmental restrictions [8]. As a consequence, the system's performance suffers. Thus, depending on the type of services and data, it is necessary to apply unique security

solutions at sensitive data levels to balance our system's performance and trust.

Mobility Node movement complicates the application of location-based methods. Furthermore, relocating and communicating with new roadside units increases the risk of attack and the presence of malicious nodes. Changing the connection increases the need for control operations, increasing the system's cost [13, 77]. To this end, it is recommended that nodes' identities be updated periodically at the system level to reduce the risk of malicious nodes and different communication levels, implement control strategies appropriate for each level, and consider the cost slightly reduced.

Heterogeneity Node heterogeneity should be considered when developing security policies and mechanisms, just as communication and networking protocols may need to be considered when developing mechanisms and constraints. There is no single protocol for the IoV environment [4, 78].

Resource management Authors in [79] presented a framework based on SDN for intelligent networks to cover safety and security. This method focused on energy consumption management. Trust management can be a challenge in the IoT environment. This issue should be considered when adopting blockchain-based solutions in processing control and load balancing at the network level. The network-processed transactions in terms of time, processed data volume, data storage, and bandwidth consumption control in consensus solutions are recognized as the factors that affect resource management and computational consumption costs when using the blockchain [2, 8, 80]. The volume of data transmitted at the system and the network level is large and diverse; this can be a source of an attack, and implementing security mechanisms is costly. It should be noted that some resources only address a specific layer of systems [81, 82]. Resources should be considered at all levels and all layers.

Blockchain standardization Blockchain standardization has not yet been done. Standards, protocols, and rules are unclear. Moreover, the heterogeneity of communication, networks, and resources in the IoV may make this challenge more manifest. Sometimes, it may prevent its implementation or cause failure [83].

6 Conclusion

Regarding the system's structure, limited resources, and heterogeneity of network nodes, as well as the critical data that circulates from users at the system level, the IoV presents various security and privacy challenges, including data management, data sharing, management, node identity, and access control. Numerous technologies are used to meet these requirements, and several blockchain-based solutions have been introduced in recent years.

This paper provided a comprehensive systematic survey of the blockchain and IoV integration for trust management. These methods can be reviewed from three general views: architecture, data, and communication. The research studies' strengths and weaknesses were discussed. According to the literature review discussions, data management methods have the highest rate of trust management approaches at 50%. The implementation tool used Hyperledger in 38% of previous studies to mimic the technique. The cost, time, performance, and fault management parameters must be considered. According to our research, the most critical evaluation parameter for blockchain-based methods is time, including system-level service-related time parameters and solution implementation time. The issues connected with integrating blockchain in the IoV were recognized based on the methodologies that have been investigated, and solutions to solve these challenges should be addressed.

In the future, with opportunities for groundbreaking research, particularly in developing more sophisticated trust models that leverage blockchain technology. These models should assess the trustworthiness of entities participating in IoV networks. Researchers must consider security and privacy for trust management solutions and combine approaches like dynamic sharding and federated learning with blockchain to address data security concerns in IoV trust management and assign trust values to nodes based on their interactions, limiting the impact of malicious behaviors.

Acknowledgements Not applicable.

Author contributions Shirin Abbasi: Investigation, Writing – original draft, Visualization, Methodology, Software. Navid Khaledian: Investigation, Preparation. Amir Masoud Rahmani: Conceptualization, Validation, Supervision.

Funding No funding was received.

Data availability No datasets were generated or analysed during the

current study.

Declarations

Ethical approval and consent to participate Not applicable.

Consent for publication Not applicable.

Human and Animal Ethics Not applicable.

Conflicts of interest There is no conflict of interest.

References

1. Sleem, L., Noura, H.N., Couturier, R.: Towards a secure ITS: Overview, challenges, and solutions. J. Inform. Secur. Appl. **55** (2020). https://doi.org/10.1016/j.jisa.2020.102637
2. Hammoud, A., Sami, H., Mourad, A., Otrok, H., Mizouni, R., Bentahar, J.: Blockchain, and Vehicular Edge Computing for Smart and Secure IoV: Challenges and directions. IEEE Internet Things Magazine. **3**(2), 68–73 (2020). https://doi.org/10.1109/IOTM.0001.1900109
3. Miglani, A., Kumar, N.: Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review. Comput. Commun. **178**, 37–63 (2020). https://doi.org/10.1016/j.comcom.2021.07.009
4. Bodkhe, U., Tanwar, S.: Secure data dissemination techniques for IoT applications: Research challenges and opportunities. Software: Pract. Experience. **51**(12), 2469–2491 (2021). https://doi.org/10.1002/spe.2811
5. Gao, L., Wu, C., Yoshinaga, T., Chen, X., Ji, Y.: Multi-channel Blockchain Scheme for Internet of vehicles. IEEE Open. J. Comput. Soc. **2**, 192–203 (2021). https://doi.org/10.1109/OJCS.2021.3070714
6. Astarita, V., Giofrè, V.P., Guido, G., Vitale, A.: The use of a blockchain-based System in Traffic operations to promote Cooperation among Connected vehicles. Procedia Comput. Sci. **177**, 220–226 (2020). https://doi.org/10.1016/j.procs.2020.10.031
7. Bhushan, B., Khamparia, A., Sagayam, K.M., Sharma, S.K., Ahad, M.A., Debnath, N.C.: Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustainable Cities Soc. **61**, p102360 (2020). https://doi.org/10.1016/j.scs.2020.102360
8. Shah, K., Chadotra, S., Tanwar, S., et al.: Blockchain for IoV in 6G environment: Review solutions and challenges. Cluster Comput. **25**, 1927–1955 (2022). https://doi.org/10.1007/s10586-021-03492-0
9. Rejeb, A., Rejeb, K., Simske, S.J., Keogh, J.G.: Blockchain technology in the smart city: A bibliometric review. Qual. Quant. 1–32 (2021). https://doi.org/10.1007/s11135-021-01251-2
10. Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P., Aski, V.J.: Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. Int. J. Commun Syst. **33**(12), e4443 (2021). https://doi.org/10.1002/dac.4443
11. Elghaish, F., Hosseini, M.R., Matarneh, S., Talebi, S., Wu, S., Martek, I., Poshdar, M., Ghodrati, N.: Blockchain and the 'Internet of things' for the construction industry: Research trends and opportunities. Autom. Constr. **132**, 103942 (2021). https://doi.org/10.1016/j.autcon.2021.103942
12. Hemmati, A., Zarei, M., Souri, A.: Blockchain-based internet of vehicles (BIoV): A systematic review of surveys and reviews. Secur. Priv. **6**, 6 (2023). https://doi.org/10.1002/spy2.317
13. Kapassa, E., Themistocleous, M.: Blockchain Technology Applied in IoV demand response management: A systematic literature. Rev. Future Internet. **14**(5) (p.136, 2022). https://doi.org/10.3390/fi14050136
14. Wang, C., Cheng, X., Li, J., et al.: A survey: Applications of blockchain in the Internet of vehicles. J. Wirel. Com. Netw. **77** (2021). https://doi.org/10.1186/s13638-021-01958-8
15. Bhushan, B., Sahoo, C., Sinha, P., Khamparia, A.: Unification of Blockchain and Internet of things (BIoT): Requirements, working model, challenges and future directions. Wireless Netw. **27**(1), 55–90 (2021). https://doi.org/10.1007/s11276-020-02445-6
16. Rahman, A., Nasir, M.K., Rahman, Z., Mosavi, A., Shahab, S., Minaei-Bidgoli, B.: Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management. IEEE Access., **8**, pp.140008–140018, https://doi.org/10.1109/ACCESS.2020.3012435
17. Villamil, S., Hernández, C., Tarazona, G.: An overview of internet of things. Telkomnika (Telecommunication Comput. Electron. Control), **18**(5), pp.2320–2327, https://doi.org/10.12928/telkomnika.v18i5.15911
18. Rahman, A., Islam, M.J., Rahman, Z., Reza, M.M., Anwar, A., Mahmud, M.P., Nasir, M.K., Noor, R.M.: Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium'. IEEE Access. **8**, 209594–209609 (2020). https://doi.org/10.1109/ACCESS.2020.3039113
19. Saxena, S., Bhushan, B., Ahad, M.A.: Blockchain based solutions to secure IoT: Background, integration trends and a way forward. J. Netw. Comput. Appl. **181**, 103050 (2021). https://doi.org/10.1016/j.jnca.2021.103050
20. Liu, Y., Wang, J., Wan, Z.Y.Z., Riku, Jäntti: A survey on blockchain-based trust management for internet of things. IEEE Internet Things J. **10**(7), 5898–5922 (2023). https://doi.org/10.1109/JIOT.2023.3237893
21. Kumar, R., Sharma, R.: Leveraging blockchain for ensuring trust in IoT: A survey. J. King Saud University-Computer Inform. Sci. (2021). https://doi.org/10.1016/j.jksuci.2021.09.004
22. Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., Yu, S.: Attacks and defences on intelligent connected vehicles: A survey. Digit. Commun. Networks. **6**(4), 399–421 (2020). https://doi.org/10.1016/j.dcan.2020.04.007
23. Mollah, M.B., Zhao, J., Niyato, D., Guan, Y.L., Yuen, C., Sun, S., Lam, K.Y., Koh, L.H.: Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. IEEE Internet Things J. **8**(6), 4157–4185 (2020). https://doi.org/10.1109/JIOT.2020.3028368
24. Rahman, A., Montieri, A., Kundu, D., Karim, M.R., Islam, M.J., Umme, S.: Alfredo Nascita, and Antonio Pescapé. On the integration of blockchain and sdn: Overview, applications, and future perspectives. J. Netw. Syst. Manage. **30**(4), 73 (2022)
25. Abbasi, S., Rahmani, A.M., Balador, A.: Internet of vehicles: Architecture, services, and applications. Int. J. Commun Syst. **34**, 10 (2021). https://doi.org/10.1002/dac.4793
26. Liu, Xuyang, K.H., Lam, K., Zhu, C., Zheng, X., Li, Y., Du, C., Liu, Philip, W.T.P.: Overview of spintronic sensors with internet of things for smart living. IEEE Trans. Magn. **55**(11), 1–22 (2019). https://doi.org/10.1109/TMAG.2019.2927457
27. Contreras-Castillo, J., Zeadally, S., Juan Antonio Guerrero-Ibañez: Internet of vehicles: Architecture, protocols, and security. IEEE Internet Things J. **5**(5), 3701–3709 (2017). https://doi.org/10.1109/JIOT.2017.2690902
28. Wijesundara, W.M.A.B., Lee, J.-S., Tith, D., Aloupogianni, E.: Hiroyuki Suzuki, and Takashi Obi. Security-enhanced firmware management scheme for smart home IoT devices using distributed ledger technologies. Int. J. Inf. Secur. : 1–11. (2024)

29. Micale, D., Matteucci, I., Fenzl, F.: Roland Rieke, and Giuseppe Patanè. A context-aware on-board intrusion detection system for smart vehicles. Int. J. Inf. Secur. : 1–21. (2024)
30. Mundhe, P., Verma, S., Venkatesan, S.: A comprehensive survey on authentication and privacy-preserving schemes in VANETs. Comput. Sci. Rev. **41**, 100411 (2021). https://doi.org/10.1016/j.cosrev.2021.100411
31. Rahman, A., Chakraborty, C., Anwar, A., et al.: SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic. Cluster Comput. **25**, 2351–2368 (2022). https://doi.org/10.1007/s10586-021-03367-4
32. Çaldağ, M.T., Gökalp, E.: Exploring critical success factors for blockchain-based intelligent transportation systems. Emerg. Sci. J. **4**, 27–44 (2020). https://doi.org/10.28991/esj-2020-SP1-03
33. Rahman, A., Hasan, K., Kundu, D., Islam, M.J., Debnath, T., Band, S.S., Neeraj Kumar: On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Comput. Syst. **138**, 61–88 (2023)
34. Shahmirzadi, D., Khaledian, N., and Amir Masoud Rahmani:. Analyzing the impact of various parameters on job scheduling in the Google cluster dataset. Cluster Comput. : 1–15. (2024)
35. Khaledian, N., Nazari, A., Khamforoosh, K., Abualigah, L., Javaheri, D.: TrustDL: Use of trust-based dictionary learning to facilitate recommendation in social networks. Expert Syst. Appl. **228**, 120487 (2023)
36. Abidi, R., Azzouna, N.B., Trojet, W., Hoblos, G., Sahli, N.: A study of mechanisms and approaches for IoV trust models requirements achievement. J. Supercomputing. **80**(3), 4157–4201 (2024)
37. Shi, K., Zhu, L., Zhang, C., Xu, L., Gao, F.: Blockchain-based multimedia sharing in vehicular social networks with privacy protection. Multimedia Tools Appl. **79**(11), 8085–8105 (2020). https://doi.org/10.1007/s11042-019-08284-8
38. Eddine, M.S., Ferrag, M.A., Friha, O., Maglaras, L.: EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. J. Inform. Secur. Appl. **59**(102802) (2021). https://doi.org/10.1016/j.jisa.2021.102802
39. Elkhalil, A., Zhang, J., Elhabob, R.: An efficient heterogeneous blockchain-based online/offline signcryption systems for internet of vehicles. Cluster Comput. **24**(3), 2051–2068 (2021). https://doi.org/10.1007/s10586-021-03246-y
40. Bagga, P., Sutrala, A.K., Das, A.K., Vijayakumar, P.: Blockchain-based batch authentication protocol for Internet of vehicles. J. Syst. Architect. **113**(101877) (2021). https://doi.org/10.1016/j.sysarc.2020.101877
41. Meng, X., Xu, J., Liang, W., Xu, Z., Li, K.C.: A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles, Computers and Electrical Engineering, vol. 95, p.107431, (2021). https://doi.org/10.1016/j.compeleceng.2021.107431
42. Singh, M., Kim, S.: Branch based blockchain technology in intelligent vehicle. Comput. Netw. **145**, 219–231 (2018). https://doi.org/10.1016/j.comnet.2018.08.016
43. Salim, M.M., Shanmuganathan, V., Loia, V., Park, J.H.: Deep learning enabled secure IoT handover authentication for blockchain networks. Hum. Cent. Comput. Inf. Sci. **11**(21) (2021). https://doi.org/10.22967/HCIS.2021.11.021
44. Vishwakarma, L., Nahar, A.: Lbsv: Lightweight blockchain security protocol for secure storage and communication in sdn-enabled Iov. IEEE Trans. Veh. Technol. **71**(6), 5983–5994 (2022). https://doi.org/10.1109/TVT.2022.3163960
45. Zhang, L., Luo, M., Li, J., Au, M.H., Choo, K.K.R., Chen, T., Tian, S.: Blockchain based secure data sharing system for internet of vehicles: A position paper. Veh. Commun. **16**, 85–93 (2019). https://doi.org/10.1016/j.vehcom.2019.03.003
46. Zhang, H., Liu, J., Zhao, H., Wang, P., Kato, N.: Blockchain-based trust management for internet of vehicles. IEEE Trans. Emerg. Top. Comput. **9**(3), 1397–1409 (2020). https://doi.org/10.1109/TETC.2020.303353
47. Wang, W., Wu, L., Qu, W., Liu, Z., Wang, H.: Privacy-preserving cloud-fog–based traceable road condition monitoring in VANET. Int. J. Network Manage. **31**(2), e2096 (2021). https://doi.org/10.1002/nem.2096
48. Wang, S., Yingnan Hu, and, Qi, G.: Blockchain and deep learning based trust management for Internet of vehicles. Simul. Model. Pract. Theory. **120**, 102627 (2022). https://doi.org/10.1016/j.simpat.2022.102627
49. Karim, S.M., Habbal, A., Chaudhry, S.A., Irshad, A.: BSDCE-IoV: Blockchain-based Secure Data Collection and Exchange Scheme for IoV in 5G environment. IEEE Access. (2023). https://doi.org/10.1109/ACCESS.2023.3265959
50. Tu, S., Yu, H., Badshah, A., Waqas, M., Halim, Z., Ahmad, I.: Secure Internet of vehicles (IoV) with decentralized Consensus Blockchain mechanism. IEEE Trans. Veh. Technol. (2023). https://doi.org/10.1109/TVT.2023.3268135
51. Abdussami, M., Dwivedi, S.K., Obaidat, M.S., Amin, R., Vollala, S.: and Balqies Sadoun. Cryptanalysis and Improvement of a Blockchain Based Lightweight Authentication and Key Agreement Scheme for Internet of Vehicles. In 2023 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), pp. 1–6. IEEE, (2023). https://doi.org/10.1109/CCCI58712.2023.10290821
52. Devi, A., Rathee, G., Saini, H.: Secure blockchain-internet of vehicles (B-IoV) mechanism using DPSO and M-ITA algorithms. J. Inform. Secur. Appl. **64**, 103094 (2022). https://doi.org/10.1016/j.jisa.2021.103094
53. Yuan, M., Xu, Y., Zhang, C., Tan, Y., Wang, Y., Ren, J., Zhang, Y.: IEEE Trans. Intell. Transp. Syst. **24**(3), 3489–3500 (2022). https://doi.org/10.1109/TITS.2022.3226500 TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Control in Internet of Vehicles.
54. Khalid, A., Iftikhar, M.S., Almogren, A., Khalid, R., Afzal, M.K., Javaid, N.: A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs. Inf. Process. Manag. **58**(2), 102464 (2021). https://doi.org/10.1016/j.ipm.2020.102464
55. Singh, S.K., Azzaoui, A.E., Kim, T.W., Pan, Y., Park, J.H.: DeepBlockScheme: A deep learning-based blockchain driven scheme for secure smart city. Hum. -Centric Comput. Inf. Sci. **11**(12) (2021). https://doi.org/10.22967/HCIS.2021.11.012
56. Lai, C., Du, Y., Guo, Q., Zheng, D.: A trust-based privacy-preserving friend matching scheme in social internet of vehicles. Peer-to-Peer Netw. Appl. **14**(4), 2011–2025 (2021). https://doi.org/10.1007/s12083-021-01140-3
57. Zhang, H., Liu, J., Zhao, H., Wang, P., Kato, N.: Blockchain-based trust management for internet of vehicles. IEEE Trans. Emerg. Top. Comput. **9**(3), 1397–1409 (2020). 2010.1109/TETC.2020.3033532
58. Singh, S., Kumar, P.K., Sharma, Y., Pan, Jong Hyuk Park: BIIoVT: Blockchain-based secure storage architecture for intelligent internet of vehicular things. IEEE Consum. Electron. Mag. (2021). https://doi.org/10.1109/MCE.2021.3089992
59. Dwivedi, S.K., Amin, R., Vollala, S., Chaudhry, R.: Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. Comput. Electr. Eng. **86**(106719) (2020). https://doi.org/10.1016/j.compeleceng.2020.106719
60. Kudva, S., Badsha, S., Sengupta, S., Khalil, I., Albert Zomaya: Towards secure and practical consensus for blockchain based VANET. Inf. Sci. **545**, 170–187 (2021). https://doi.org/10.1016/j.ins.2020.07.060

61. Gawas, M., Patil, H., Govekar, S.S.: An integrative approach for secure data sharing in vehicular edge computing using Blockchain. Peer-to-Peer Netw. Appl. **14**(5), 2840–2857 (2021). https://doi.org/10.1007/s12083-021-01107-4
62. Mershad, K., Cheikhrouhou, O., Ismail, L.: Proof of accumulated trust: A new consensus protocol for the security of the IoV. Veh. Commun. **32**(100392) (2021). https://doi.org/10.1016/j.vehcom.2021.100392
63. Ahmad, F., Kerrache, C.A., Kurugollu, F., Hussain, R.: Realization of blockchain in named data networking-based internet-of-vehicles. I T Prof. **21**(4), 41–47 (2019). 2010.1109/MITP.2019.2912142
64. Khelifi, H., Luo, S., Nour, B., Moungla, H., Ahmed, S.H., Guizani, M.: Comput. Electr. Eng. **86**(106715) (2020). https://doi.org/10.1016/j.compeleceng.2020.106715 A blockchain-based architecture for secure vehicular Named Data Networks
65. Meng, X., Xu, J., Liang, W., Xu, Z., Li, K.C.: A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles. Comput. Electr. Eng. **95**, 107431 (2021). https://doi.org/10.1016/j.compeleceng.2021.107431
66. Xu, Z., Liang, W., Li, K.C., Xu, J., Jin, H.: A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. J. Parallel Distrib. Comput. **149**, 29–39 (2021). https://doi.org/10.1016/j.jpdc.2020.11.003
67. Rahman, A., Khan, M.S.I., Montieri, A., Islam, M.J.: Md Razaul Karim, Mahedi Hasan, Dipanjali Kundu, Mostofa Kamal Nasir, and Antonio Pescapè. BlockSD-5GNet: Enhancing security of 5G network through blockchain-SDN with ML-based bandwidth prediction. Trans. Emerg. Telecommunications Technol. **35**(4), e4965 (2024)
68. Kumar Arora, Sandeep, G., Kumar, M., Hedabou, E.M., Amhoud, Iwendi, C.: Blockchain-inspired lightweight trust-based system in vehicular networks. Int. J. Network Manage. e2226 (2023). https://doi.org/10.1002/nem.2226
69. Oham, C., Michelin, R.A., Jurdak, R., Kanhere, S.S., Jha, S.: B-FERL: Blockchain based framework for securing smart vehicles. Inf. Process. Manag. **58**(1) (p.102426, 2021). https://doi.org/10.1016/j.ipm.2020.102426
70. Jiang, M., Wang, H., Zhang, W., Qin, H., Sun, X.: Comput. Electr. Eng. **86**(106716) (2020). https://doi.org/10.1016/j.compeleceng.2020.106716 Location-based data access control scheme for Internet of Vehicles
71. Sun, L., Yang, Q., Chen, X., Chen, Z.: RC-chain: Reputation-based crowdsourcing blockchain for vehicular networks. J. Netw. Comput. Appl. **176**(102956) (2021). https://doi.org/10.1016/j.jnca.2020.102956
72. Rathore, S., Park, J.H., Chang, H.: Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. IEEE Access. **9**, 90075–90083 (2021). https://doi.org/10.1109/ACCESS.2021.3077069
73. Cheng, G., Huang, J., Wang, Y., Zhao, J., Kong, L., Deng, S.: Conditional privacy-preserving Multi-domain Authentication and Pseudonym Management for 6G-Enabled IoV. IEEE Trans. Inf. Forensics Secur. (2023). https://doi.org/10.1109/TIFS.2023.3314211
74. Singh, U., Sharma, S.K., Shukla, M.: and Preeti Jha. Blockchain-based BATMAN protocol using mobile ad hoc network (MANET) with an ensemble algorithm. Int. J. Inf. Secur. : 1–11. (2024)
75. Chattaraj, D., Bera, B., Das, A.K., Saha, S., Lorenz, P., Park, Y.: Block-CLAP: Blockchain-assisted Certificateless Key Agreement Protocol for Internet of vehicles in Smart Transportation. IEEE Trans. Veh. Technol. (2021). https://doi.org/10.1109/TVT.2021.3091163
76. Abirami, G.: Performance analysis of the dynamic trust model algorithm using the fuzzy inference system for access control. Comput. Electr. Eng. **92**, 107132 (2021)
77. Javaid, U., Aman, M.N., Sikdar, B.: A scalable protocol for driving trust management in internet of vehicles with blockchain. IEEE Internet Things J. **7**(12), 11815–11829 (2020). https://doi.org/10.1109/JIOT.2020.3002711
78. Akraminejad, R., Khaledian, N., Nazari, A., Voelp, M.: A multi-objective crow search algorithm for optimizing makespan and costs in scientific cloud workflows (CSAMOMC). Computing, 1–17. (2024)
79. Rahman, A., Islam, M.J., Montieri, A., Nasir, M.K., Reza, M.M., Band, S.S., Pescape, A., Hasan, M., Sookhak, M., Mosavi, A.: Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot. IEEE Access. **9**, 28361–28376 (2021). https://doi.org/10.1109/ACCESS.2021.3058244
80. Islam, M.J., Rahman, A., Kabir, S., Karim, M.R., Acharjee, U.K., Nasir, M.K., Band, S.S., Sookhak, M., Wu, S.: Blockchain-SDN-Based energy-aware and distributed Secure Architecture for IoT in Smart cities. IEEE Internet Things J. **9**(5), 3850–3864 (2021). https://doi.org/10.1109/JIOT.2021.3100797
81. Xu, L., Ge, M., Wu, W.: Edge server deployment scheme of blockchain in IoVs. IEEE Trans. Reliab. **71**(1), 500–509 (2022). https://doi.org/10.1109/TR.2022.3142776
82. Hosseinzadeh, M., Abbasi, S., Amir Masoud Rahmani: Resource Manage. Approaches Internet Veh. Multimedia Tools Appl. **82**(30), 46811–46844 (2023)
83. Xu, Y., Liu, Z., Zhang, C., Ren, J., Zhang, Y., Shen, X.: Blockchain-Based Trustworthy Energy Dispatching Approach for high renewable energy penetrated Power systems. IEEE Internet Things J. **9**(12), 10036–10047 (2022). https://doi.org/10.1109/JIOT.2021.3117924